Kyberturvallisuus osana liiketoimintaa

Panosta tietoturvaan – pidä bisnes ja yhteiskunnan toiminnot käynnissä NIS2-direktiivin vaatimusten mukaan.

Mikä on NIS2-direktiivi?

NIS2-direktiivi on osa EU:n strategiaa, jonka tarkoituksena on suojella digitaalista infrastruktuuria ja parantaa alueen yhteistä turvallisuutta kyberturvallisuuden osalta alati muuttuvassa maailmassa. Direktiivi kuuluu kyberturvallisuuden riskienhallintaan liittyvää lakiin, jonka eduskunta käsittelee vuoden 2024 ensimmäisellä puoliskolla. Kyberturvallisuus kuuluu tietohallinnan kokonaisuuteen.

Direktiivi edellyttää eri alojen toimijoilta tietoturvastandardien noudattamista sekä varautumista kyberuhkiin ja niiden torjumista niin, että ihmisten arjen kannalta kriittiset toiminnot yhteiskunnassa eivät horju.

Aluksi vaatimukset ja edellytykset koskettavat valtion infrastruktuurin ja toimintavalmiuden kannalta kriittisiä aloja:

KESKEISET ALAT:

Energia
Kuljetus
Pankkitoiminta
Rahoitusmarkkinoiden infrastruktuuri
Terveysala
Juomavesi
Jätevesi
Digitaalinen infrastruktuuri
IT-palveluiden hallinta
Julkishallinto
Avaruus

TÄRKEÄT ALAT:

Posti- ja kuriiripalvelut
Jätehuolto
Kemikaalit
Ruoka
Lääkinnällisten laitteiden valmistus
Digitaaliset palveluntarjoajat
Tutkimusorganisaatiot

Direktiivi astuu voimaan lokakuussa 2024, jolloin tärkeillä aloilla toimivien yritysten dokumentointi ja varautuminen kyberturvallisuusuhkiin tulee suunniteltu.

Mikäli yritykseen kohdistuu kyberhyökkäys eikä direktiivin mukainen dokumentointi ja toimenpidesuunnitelma ole kunnossa, vastaa yrityksen johto rikkeestä aiheutuvasta sakosta henkilökohtaisesti.

Summa voi olla jopa 2 % yrityksen liikevaihdosta. Direktiivin noudattamatta jättämisestä voi siis seurata vakavia henkilökohtaisia taloushaasteita ja mainehaittaa yritykselle.

Mitä tehdä? – askeleet kohti pitävää tietoturvaa

Kyberturvallisuus osana tietohallintaa muodostaa hyvin ja selkeästi johdettuna ja suunniteltuna selkärangan yrityksen menestykselle ja tuloksentekokyvylle. Uusi direktiivi ja laki velvoitteineen mahdollistaa ydinosaamisalueeseen keskittymisen ja kansalaisten arjen pyörimisen mahdollista kyberturvallisuusuhkista huolimatta. Tietoturva ei ole vain uhkien torjuntaa, se on osa liiketoimintaa ja sen kehittämistä.

Kyberturvallisuusriskien minimointi on jaettu viiteen osaan, jotka yrityksen johtoportaan tulee dokumentoida.

ASIAA VOI LÄHESTYÄ LUOTTOKORTTIESIMERKIN KAUTTA:

Jos omistat luottokortin ja säilytät sitä lompakossasi, kannattaa kortin pin-koodi säilyttää jossain muualla. Jos korttisi katoaa, selviät kadonneen kortin kuolettamisella ja uuden kortin hankinnalla sen sijaan, että joku muu pääsisi käsiksi pankkitiliisi.

5 askelta pitävään tietoturvaan

Kaikkien kohtien tulee olla huomioitu asianmukaisesti. Direktiiviä ja kybertietoturvan riskienhallintalakia valvovat viranomaiset.

1. Riskien tunnistaminen

Kaikki alkaa alkukartoituksesta: Tunnistaako yritys sen toimintaan liittyvät tietoturvariskit liittyen niin työntekijöihin, viestintään, laitteistoon, ohjelmistoihin, tiedon säilyttämiseen, tunnuksiin ja esimerkiksi tietojen varastointiin? Onko asiat dokumentoitu asianmukaisesti?

2. Suojautuminen

Kun mahdolliset riskit on tunnistettu, on niiltä suojauduttava asianmukaisesti. Toimenpiteet tulee dokumentoida ja pitää ajan tasalla eri osa-alueilla.

3. Havainnointi

Jos kyberuhka havaitaan, tulee uhkaa seuraavien toimenpiteiden olla dokumentoitu ja suunniteltu, jotta tieto uhasta saavuttaa asiasta vastaavat henkilöt ja uhkaan vastaaminen voi alkaa.

4. Reagointi

Uhkan havaitsemisen jälkeen suunnitellut toimet voidaan suorittaa oikea-aikaisesti ja minimoida uhkasta aiheutuva haitta niin yritykselle kuin kansalaisille. Selkeä toimenpidesuunnitelma on äärimmäisen tärkeää. Esimerkiksi: pystyykö yritys toimimaan, jos sen tiedot otetaan haltuun ja kryptataan ulkopuolisen toimesta ja vaaditaan esimerkiksi lunnaita tietojen palauttamiseksi?

5. Palautuminen

Poikkeaman jälkeen dokumentoidun toimintasuunnitelman mukaan toimiminen auttaa palaamaan takaisin normaaliin arkeen ja yritystoimintaan sekä parantamaan tietoturvaa entisestään.

Grant Thorntonin tilanne- ja riskientunnistusanalyysin avulla saat kattavan kokonaiskuvan yrityksesi tietoturvasta ja vaadittavista toimenpiteistä.

Tämän pohjalta prosessien ja käytänteiden tehostaminen on helpompaa – olemme tässä apunasi.

Lopputuloksena syntyvän dokumentaatio ottaa huomioon toimialakohtaiset kyberturvallisuusuhat ja priorisoida niihin vastaamiseen. Tehtyjen toimien pohjalta kyberturvallisuustyötä kehitetään jatkuvasti, sillä kansallinen turvallisuustilanne on muuttunut viime vuosina. Uhkat ovat siis todellisia.

Miksi valita Grant Thornton?

Grant Thorntonilta saat pitkän kokemuksen ja monipuolisen tietohallintoasiantuntemuksen lisäksi kustannustehokkuuden ja maailmanlaajuisen asiantuntijaverkoston, joka käsittää tarvittaessa yli 70 000 ammattilaista ympäri maailman.

Organisaatio on iso, mutta ketterä ja nopea. Grant Thornton sitoutuu asiakkaaseen ja kilpailee laadulla. Yksittäisen projektin lisäksi yhteistyö on mahdollista toteuttaa jatkuvana, esimerkiksi kerran kuussa toteutettavana sparrauksena. Pitkä kokemus riskienhallinnasta muuttuvassa ympäristössä on kaiken a ja o.

Erityisesti moni pieni ja keskisuuri yritys pystyisi pienellä paneutumisella ja selkeän suunnitelman pohjalta saavuttamaan tietoturvallisemman ympäristön.

Oletko sinä yksi heistä?

Ota yhteyttä:

Joachim von Schantz

CIO

joachim.von.schantz@fi.gt.com
+358 505669373

Grant Thornton kuuluu maailman johtaviin tilintarkastus-, vero-, yritysjärjestely- ja muita asiantuntijapalveluita tarjoaviin yrityksiin. Asiantuntijamme auttavat dynaamisia organisaatiota kasvamaan tarjoamalla kattavia, mielekkäitä ja tulevaisuuteen suuntautuneita neuvontapalveluita.

Palvelemme asiakkaitamme Suomessa ja kansainvälisesti Helsingin ja Turun toimistoiltamme käsin.

Kiitos!

Grant Thornton

grantthornton.fi